

# Abnormal Subspace Sparse PCA for Anomaly Detection and Interpretation

Xingyan Bin  
Tsinghua University  
Beijing, China  
bxy13  
@mails.tsinghua.edu.cn

Ying Zhao<sup>\*</sup>  
Tsinghua University  
Beijing, China  
yingz  
@mail.tsinghua.edu.cn

Bilong Shen  
Tsinghua University  
Beijing, China  
shenbl12  
@mails.tsinghua.edu.cn

## ABSTRACT

The main shortage of principle component analysis (PCA) based anomaly detection models is their interpretability. In this paper, our goal is to propose an interpretable PCA-based model for anomaly detection and interpretation. The proposed ASPCA model constructs principal components with sparse and orthogonal loading vectors to represent the abnormal subspace, and uses them to interpret detected anomalies. Our experiments on a synthetic dataset and two real world datasets showed that the proposed ASPCA models achieved comparable detection accuracies as the PCA model, and can provide interpretations for individual anomalies.

## Keywords

Anomaly detection, PCA, Anomaly interpretation, sparsity, optimization

## 1. INTRODUCTION

Principal Component Analysis (PCA) is one of the best-known statistical analysis techniques for detecting anomalies and has been applied to many kinds of data, such as network intrusion detection, failure detection in production systems, and so on [4, 21, 16, 11]. In these domains, pinpointing the sources of detected anomalies is also very important for real applications such as diagnosing failures and recovering systems/networks. Hence, for each detected anomaly, an ideal model should also be able to interpret the reasons of its detection, which we refer to as the problem of **anomaly interpretation**.

Traditional PCA-based anomaly detection models are not suitable for anomaly interpretation [22, 17], as they judge whether a data instance is an anomaly or not based on the length of its projection on the abnormal subspace spanned by the less significant principal components, and there is no

direct mapping between PCA's dimensionality-reduced subspace and the original feature space. Existing approaches [22] added a separated interpretation step to solve this problem by using techniques such as decision trees. However such indirect interpretation often failed to reveal the true causes of the anomalies detected by PCA-based methods [17]. Another recent work [11] proposed the joint sparse PCA (JSPCA) model to identify a low-dimensional approximation of the abnormal subspace, so that *all* anomalies can be *localized* onto a small subset of original feature variables. However, for individual anomaly interpretation, especially anomalies of different types, we need a more accurate and direct way of interpretation.

This paper aims to design an interpretable PCA-based anomaly detection model. Our key observation is that if we manage to construct principal components (PCs) with *sparse* and *orthogonal* loading vectors to represent the abnormal subspace, a detected anomaly can be interpreted by identifying the set of such PCs on which the anomaly has large projection values. We propose interpretable **Abnormal subspace sparse PCA (ASPCA)** models for anomaly detection and interpretation in this paper, and make the following two contributions.

First, we formulate two objective functions for ASPCA: one extracts the most significant sparse orthogonal PCs first, and the other extracts the least significant sparse orthogonal PCs first, which prioritizes the sparsity of the abnormal subspace. To the best of our knowledge, the proposed ASPCA models are the first PCA-based models that are suitable for individual anomaly detection and interpretation. Second, we propose an optimization method for ASPCA models with a semidefinite programming (SDP) relaxation step and a global sparsity optimization step. Our experiments on a synthetic dataset and two real world datasets showed that the proposed ASPCA models achieved comparable detection accuracies as the PCA model, and can provide interpretations for individual anomalies.

The rest of this paper is organized as follows. Section 2 introduces the proposed ASPCA models. Section 3 describes the optimization methods for ASPCA models. Section 4 presents a comprehensive experimental evaluation. Section 5 discusses the related work. Finally, Section 6 provides some concluding remarks.

## 2. RELATED WORK

PCA is mostly known as a dimension reduction tool [12], but it is also widely used as an anomaly detection method

<sup>\*</sup>Corresponding author

[6, 4]. Wei Xu *et al.* used this technique to analyze logs and detect anomalies on a game server, Hadoop File System (HDFS) [22], and Google’s production system [21]. Ryohi Fujimaki *et al.* used kernel PCA on the Spacecraft Anomaly Detection Problem [7]. People have implemented this technique on network intrusion detection [16, 15, 11, 19]. Anukool Lakhina *et al.* applied this technique on the problem of network flood monitoring using PCA on the matrix of time and Origin-Destination pairs [16, 15]. Firstly, they used the volume of communication [15] in their model, and then they extent their model with the entropy of communication volumes and applied PCA with multiple subspace [16]. Ling Huang *et al.* tried to design an online PCA-based detection method for scalability and communication efficiency [9, 8].

One of the major disadvantages of PCA as a dimension reduction tool is its poor interpretability. Ian Jolliffe *et al.* introduced the concept of sparse PCA which adds a constraint on the sparsity of loading vectors [13]. Since, various methods solving the sparse PCA problem were proposed in the literature, for example [23] and [5]. Hui Zou *et al.* transformed the sparse PCA problem to a regression-type problem with an elastic net regularization, which could be solved by an alternating minimization scheme [23]. Alexandre d’Aspremont *et al.* proposed a semi-definite programming (SDP) relaxation to the sparse PCA optimization problem [5].

PCA-based anomaly detection methods also suffer from the shortage of interpretability [17, 22]. Ruoyi Jiang *et al.* introduced the joint sparse PCA method for anomaly localization inspired by sparse PCA [10, 11], and they followed the alternating minimization framework [23] to solve the optimization problem [11]. Wei Xu *et al.* also tried to interpret the results returned by a PCA anomaly detection model with decision trees trained by the data labeled by the PCA model [22], which as shown in our experimental results, can be misleading and fail to reveal the true reason behind the PCA model.

### 3. PCA FOR ANOMALY DETECTION AND INTERPRETATION

#### 3.1 Notations

Bold uppercase letters such as  $\mathbf{X}$  denote a matrix and bold lowercase letters such as  $\mathbf{x}$  denote a column vector. Greek letters such as  $\lambda, \mu$  are coefficients.  $\|\mathbf{X}\|_F$  is the Frobenius norm of  $\mathbf{X}$ , and  $\|\mathbf{X}\|_{1,1}$  is the  $L_{1,1}$  norm of  $\mathbf{X}$  as  $\|\mathbf{X}\|_{1,1} = \mathbf{1}|\mathbf{X}|\mathbf{1}^T$ .

A dataset is represented as an  $n \times p$  data matrix  $\mathbf{D}$ , where each row vector corresponds to a  $p$ -dimensional data instance, and each column vector corresponds to a feature variable.  $\mathbf{A} = \mathbf{D}^T \mathbf{D}$  is  $\mathbf{D}$ ’s covariance matrix.  $Tr(\mathbf{A})$  represents the trace of matrix  $\mathbf{A}$ .  $Card(\mathbf{A})$  denotes the cardinality (number of non-zero elements) of matrix  $\mathbf{A}$ .  $\mathbf{I}$  is the identity matrix.  $\mathbb{S}^p$  is the set of all symmetric semidefinite matrices in  $\mathbb{R}^{p \times p}$ .

#### 3.2 PCA for Anomaly Detection

Principal Component Analysis (PCA) is a dimensionality-reduction technique that captures the highest variance of a multi-dimensional dataset in a lower dimensional subspace defined by a set of orthogonal eigen vectors. Given a  $p$ -dimensional dataset, a detection model can be constructed

by forming a “normal subspace” (defined by the first  $k$  principal components returned by PCA) and an “abnormal subspace” (the remaining subspace by removing the normal subspace). Since the normal subspace captures the highest variance of the dataset, PCA-based detection methods assume that this  $k$ -subspace corresponds to the normal trends of the dataset, and all normal data tends to have almost zero length projection on the abnormal subspace. Therefore, given a  $p$ -dimensional data, the model can detect whether it is an anomaly or not based on whether it is primarily expressed by the normal or abnormal subspace [17].

More formally, let  $\mathbf{V}_1 = (\mathbf{v}_1, \dots, \mathbf{v}_k)$  be the normal subspace defined by the first  $k$  principal components with  $\mathbf{v}_1, \dots, \mathbf{v}_k$  being the orthogonal loading vectors, and  $\mathbf{V}_2 = (\mathbf{v}_{k+1}, \dots, \mathbf{v}_p)$  be the abnormal subspace defined by the remaining  $p-k$  principal components with  $\mathbf{v}_{k+1}, \dots, \mathbf{v}_p$  being the orthogonal loading vectors of these PCs. Given a  $p$ -dimensional data  $\mathbf{y}$ , its residual  $\hat{\mathbf{y}}$  is defined as:

$$\hat{\mathbf{y}} = \mathbf{y} - \mathbf{V}_1 \mathbf{V}_1^T \mathbf{y}. \quad (1)$$

The squared length of  $\hat{\mathbf{y}}$ , called the squared prediction error (SPE), is the metric to indicate whether  $\mathbf{y}$  is an anomaly or not. The larger SPE is, the more likely  $\mathbf{y}$  is an anomaly.

#### 3.3 Anomaly Interpretation

When the SPE score of a given instance  $\mathbf{y}$  is over a pre-defined threshold,  $\mathbf{y}$  is considered as an anomaly. It is then important to understand where the abnormality of  $\mathbf{y}$  comes from, *i.e.*, what anomalous feature behaviors of  $\mathbf{y}$  are more responsible for distinguishing  $\mathbf{y}$  from normal data. We call this problem as **Anomaly Interpretation**. The anomaly interpretation for PCA is difficult, as there is no direct mapping between PCA’s dimensionality-reduced subspace and the original feature space for anomaly [17]. In other words, the length of  $\hat{\mathbf{y}}$  can be used to detect anomaly, whereas interpreting  $\hat{\mathbf{y}}$  directly is meaningless.

Given the normal subspace  $\mathbf{V}_1$  and abnormal subspace  $\mathbf{V}_2$ , we can rewrite  $\hat{\mathbf{y}}$  as follows:

$$\hat{\mathbf{y}} = \mathbf{y} - \mathbf{V}_1 \mathbf{V}_1^T \mathbf{y} = \mathbf{V}_2 \mathbf{V}_2^T \mathbf{y}. \quad (2)$$

To design an interpretable PCA-based anomaly detection model, we have the following proposition.

**PROPOSITION 3.1.** *Given  $\mathbf{V}_2 = (\mathbf{v}_{k+1}, \dots, \mathbf{v}_p)$ , where  $\mathbf{v}_{k+1}, \dots, \mathbf{v}_p$  are orthogonal loading vectors, SPE can be expressed by*

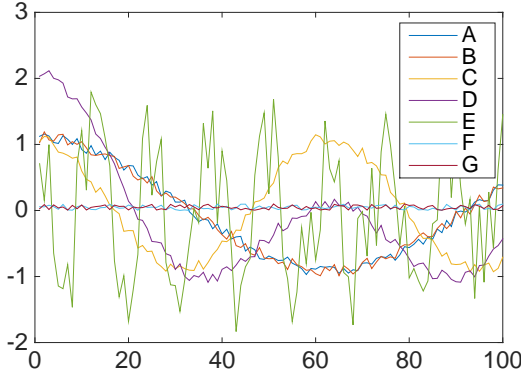
$$SPE = \hat{\mathbf{y}}^T \hat{\mathbf{y}} = \sum_{i=k+1}^p (\mathbf{v}_i^T \mathbf{y})^2. \quad (3)$$

**PROOF.**

$$\begin{aligned} SPE &= \hat{\mathbf{y}}^T \hat{\mathbf{y}} = \mathbf{y}^T \mathbf{V}_2 \mathbf{V}_2^T \mathbf{V}_2 \mathbf{V}_2^T \mathbf{y} \\ &= (\mathbf{y}^T \mathbf{V}_2) (\mathbf{V}_2^T \mathbf{V}_2) (\mathbf{V}_2^T \mathbf{y}) = (\mathbf{V}_2^T \mathbf{y})^T (\mathbf{V}_2^T \mathbf{y}) \\ &= \sum_{i=k+1}^p (\mathbf{v}_i^T \mathbf{y})^2. \end{aligned} \quad (4)$$

□

In other words, SPE is equal to the square sum of  $\mathbf{y}$ ’s scalar projection on each abnormal PCs, so that we can identify the set of PCs that are responsible for the abnormality indicated by high projection values. Unfortunately, these PCs



(a) Normal Instances of the Synthetic Data

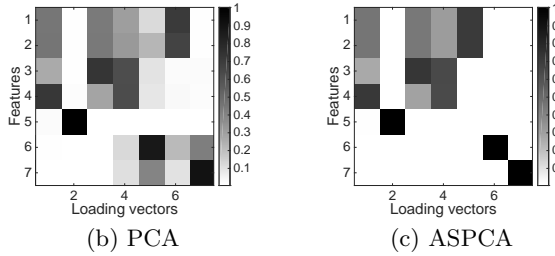


Figure 1: Synthetic data and loading matrices obtained by PCA and ASPCA

are still difficult to interpret, since each abnormal PC is complicated as it is a linear combination of all feature variables. To make them interpretable, we have to make these abnormal PCs sparse, *i.e.*, each represented by a few feature variables. Hence, our key observation is that if we manage to extract PCs with **sparse** and **orthogonal** loading vectors to represent abnormal subspace, these loading vectors can be used to detect and interpret anomalies. The orthogonality guarantees that Eqn. 4 holds, so that the abnormality can be translated to high projection values on a set of abnormal PCs, while the sparsity guarantees that these abnormal PCs are interpretable. We call the above method as the **Abnormal Subspace Sparse PCA (ASPCA)** method. Now we use an example to illustrate this idea.

We synthesized a dataset with 500 normal records and 15 anomalies (first 100 normal records are shown in Figure 1a). Each data record has 7 features named from *A* to *G*, and the normal records were generated with four patterns,  $A \approx B$ ,  $D \approx C + A$ ,  $F \approx 0$ , and  $G \approx 0$ . The anomalies were generated as three categories by breaking the first three patterns, respectively. The loading matrix of PCs obtained by PCA is shown in Figure 1b, where the last four PCs can be used to detect anomalies but difficult to interpret. Now, if we can make the loading vectors of last four PCs **sparse** and **orthogonal** as shown in Figure 1c, they can be used to detect and interpret anomalies simultaneously. Now, the interpretation of a detected anomaly can be conducted in two steps. First, we can identify the set of projections that contribute the most for a high SPE score according to Eqn. 4. Then, we can interpret these projections one by one, by identifying which original feature variables are responsible for each projection, and how each projection triggers a high SPE score.

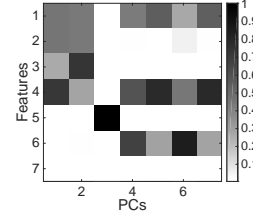


Figure 2: Loading matrix obtained by JSPCA

Recently, Jiang *et al.* [11] proposed a joint sparse PCA (JSPCA) model to achieve a sparse representation of the abnormal subspace too. The main idea was to identify a low-dimensional approximation of the abnormal subspace using a subset of feature variables, where all abnormal PCs are represented by the same subset of feature variables as shown in Figure 2. Although JSPCA can identify the set of features that distinguish the anomalies, it has two limitations that fail to meet our goals. First, the features identified by JSPCA are optimized for all anomalies as a whole. In particular, if anomalies are of different types, which is a common case for domains such as network intrusion detection or system failure detection, they should be interpreted by different sets of features inherently. As an unsupervised method, JSPCA cannot assume that anomalies in the dataset are of the same type, and cannot handle them well if they indeed are of different types. Second, JSPCA can only identify the important features for anomaly detection, but no direct interpretation as why anomalies are detected.

### 3.4 Abnormal Subspace Sparse PCA

Now we need to formulate the objective function of the Abnormal Subspace Sparse PCA (ASPCA) problem. The recently studied sparse PCA framework [5] adds a sparsity constraint on the principal components (PCs). However, we cannot use this framework directly to solve our problem. The main reason is that the sparse PCA framework usually does not enforce orthogonality on the resultant sparse PCs. Consequently, the resultant sparse PCs cannot be used to define the normal and abnormal subspaces, as the abnormal PCs are not the orthogonal complement of the normal PCs.

By enforcing orthogonality, sparse PCA can be used to solve our ASPCA problem, which we denote as *forward* ASPCA (shorted as ASPCA-F). Given a covariance matrix  $\mathbf{A}$  and a sparsity constraint constant  $k$ , for each  $i = 1, \dots, p$ , ASPCA-F tries to solve:

$$\begin{aligned} & \underset{\mathbf{v}_i}{\operatorname{argmax}} \quad \mathbf{v}_i^T \mathbf{A} \mathbf{v}_i \\ & \text{s.t.} \quad \mathbf{v}_i^T \mathbf{v}_i = 1, \mathbf{v}_i^T \mathbf{v}_j = 0 \quad \forall 1 \leq j < i, \operatorname{Card}(\mathbf{v}_i) \leq k. \end{aligned} \quad (5)$$

The last  $d$  loading vectors obtained by solving Eqn. 5 are used for detecting and interpreting anomalies.

One of the drawbacks of the ASPCA-F framework is that the last abnormal PCs tend to have poor sparsity. To solve this problem, we propose a *Backward* ASPCA framework (shorted as ASPCA-B) that extracts the least significant orthogonal PCs first, which prioritizes the optimization of the sparsity of the abnormal subspace. To see how it works, we first show that the process of standard PCA can be reversed, so that eigen vectors with smaller eigen values are extracted first by the following proposition.

PROPOSITION 3.2. Given a covariance matrix  $\mathbf{A} = \mathbf{D}^T \mathbf{D}$ , if we have already extracted the eigen vectors  $\mathbf{v}_{k+1}, \mathbf{v}_{k+2}, \dots, \mathbf{v}_n$  with the  $n-k-1$  smallest eigen values, and remaining eigen vectors are  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$  with eigen values  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$  of  $\mathbf{A}$ , the solution of Eqn. 6 is the eigen vector with the eigen value  $\lambda_k$ .

$$\begin{aligned} & \underset{\mathbf{v}}{\operatorname{argmin}} \quad \mathbf{v}^T \mathbf{A} \mathbf{v} \\ & \text{s.t. } \mathbf{v}^T \mathbf{v} = 1, \quad \mathbf{v}^T \mathbf{v}_i = 0 \quad \forall k < i \leq n \end{aligned} \quad (6)$$

PROOF. We project  $\mathbf{v}$  on  $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ ,  $\mathbf{v} = \sum_{i=1}^n \alpha_i \mathbf{v}_i = \sum_{i=1}^k \alpha_i \mathbf{v}_i$ , where  $\alpha_i = \mathbf{v}^T \mathbf{v}_i$ . As  $\mathbf{v}_i^T \mathbf{v}_j = 0, i \neq j$ , we have  $\mathbf{v}^T \mathbf{v} = \sum_{i=1}^k \alpha_i^2 = 1$ . Then,

$$\begin{aligned} & \mathbf{v}^T \mathbf{A} \mathbf{v} \\ &= \left( \sum_{i=1}^k \alpha_i \mathbf{v}_i \right) \left( \sum_{i=1}^k \alpha_i \mathbf{A} \mathbf{v}_i \right) = \left( \sum_{i=1}^k \alpha_i \mathbf{v}_i \right) \left( \sum_{i=1}^k \alpha_i \lambda_i \mathbf{v}_i \right) \\ &= \sum_{i=1}^k \alpha_i^2 \lambda_i \mathbf{v}_i^T \mathbf{v}_i + \sum_{i=1}^k \sum_{j=1, j \neq i}^k \alpha_i \alpha_j \lambda_j \mathbf{v}_i^T \mathbf{v}_j \\ &= \sum_{i=1}^k \alpha_i^2 \lambda_i \end{aligned}$$

As  $\lambda_i \geq \lambda_k, i \leq k$ , we know  $\mathbf{v}^T \mathbf{A} \mathbf{v} = \sum_{i=1}^k \alpha_i^2 \lambda_i \geq \sum_{i=1}^k \alpha_i^2 \lambda_k = \lambda_k$ . And we know  $\min_{\mathbf{v}} \mathbf{v}^T \mathbf{A} \mathbf{v} \leq \mathbf{v}_k^T \mathbf{A} \mathbf{v}_k = \lambda_k$ , so  $\min_{\mathbf{v}} \mathbf{v}^T \mathbf{A} \mathbf{v} = \lambda_k$ .

With the optimum  $\hat{\mathbf{v}} = \sum_{i=1}^k \hat{\alpha}_i \mathbf{v}_i$ , we have:

$$\begin{aligned} \lambda_k - \sum_{i=1}^k \hat{\alpha}_i^2 \lambda_i &= \sum_{i=1}^k \hat{\alpha}_i^2 (\lambda_k - \lambda_i) = 0 \\ \lambda_k - \lambda_i &\leq 0, i < k \end{aligned}$$

So, we know that  $\hat{\alpha}_i \neq 0$  only if  $\lambda_i = \lambda_k$ . Hence,  $\hat{\mathbf{v}}$  is a linear combination of the eigen vectors with eigen value  $\lambda_k$ , and  $\hat{\mathbf{v}}$  must be an eigen vector with eigen value  $\lambda_k$  too.

□

Obviously, the proposition also holds for  $k = n$ . Together we see that using Eqn. 6, eigen vectors can be calculated in an increasing order of eigen values. Now, we add a sparsity constraint to Eqn. 6 and form the objective function for our ASPCA-B framework as follows.

Given a covariance matrix  $\mathbf{A}$  and a sparsity constraint constant  $k$ , for each  $i = 1, \dots, d$ , our ASPCA-B framework tries to solve:

$$\begin{aligned} & \underset{\mathbf{v}_i}{\operatorname{argmin}} \quad \mathbf{v}_i^T \mathbf{A} \mathbf{v}_i \\ & \text{s.t. } \mathbf{v}_i^T \mathbf{v}_i = 1, \quad \mathbf{v}_i^T \mathbf{v}_j = 0 \quad \forall 1 \leq j < i, \text{Card}(\mathbf{v}_i) \leq k. \end{aligned} \quad (7)$$

When we extract  $d$  loading vectors  $\mathbf{v}_1 \dots \mathbf{v}_d$  to span a subspace  $\mathbf{S}_a$ , we make sure that the orthogonal complement of  $\mathbf{S}_a$  has major variance for describing the normal patterns in the dataset, so that  $\mathbf{S}_a$  is the abnormal subspace and the resultant  $d$  sparse principal components can be used to detect and interpret anomalies.

## 4. METHODOLOGY

We derive a solution for Eqn. 5 following the semidefinite programming (SDP) relaxation framework proposed by [5].

We then modify it to solve Eqn. 7. Finally, we further optimize the sparsity of all the obtained abnormal components with the constraint of spanning the same subspace using the alternating minimization scheme inspired by [23].

### Solving ASPCA-F with SDP Relaxation.

We first transform Eqn. 5 without the orthogonality constraint  $\mathbf{v}_j^T \mathbf{v}_i = 0, \forall 1 \leq j < i$  to Eqn.8 through a SDP relaxation.

$$\begin{aligned} & \underset{\mathbf{X}_i \in \mathbb{S}^p}{\operatorname{argmax}} \quad \operatorname{Tr}(\mathbf{A} \mathbf{X}_i) \\ & \text{s.t. } \mathbf{X}_i \succeq 0, \operatorname{rank}(\mathbf{X}_i) = 1, \operatorname{Tr}(\mathbf{X}_i) = 1, \operatorname{Card}(\mathbf{X}_i) < k^2 \end{aligned} \quad (8)$$

where  $\mathbf{X}_i$  is a positive semi-definitive matrix with the constraint  $\operatorname{rank}(\mathbf{X}_i) = 1$ , which can be uniquely decomposed as  $\mathbf{X}_i = \mathbf{v}_i \mathbf{v}_i^T$ . With  $\mathbf{X}_i = \mathbf{v}_i \mathbf{v}_i^T$ ,  $\operatorname{Tr}(\mathbf{X}_i) = 1$  is equivalent to  $\mathbf{v}_i^T \mathbf{v}_i = 1$ ,  $\operatorname{Card}(\mathbf{X}_i) \leq k^2$  is equivalent to  $\operatorname{Card}(\mathbf{v}_i) \leq k$ , and we have  $\mathbf{v}_i^T \mathbf{A} \mathbf{v}_i = \operatorname{Tr}(\mathbf{A}(\mathbf{v}_i \mathbf{v}_i^T)) = \operatorname{Tr}(\mathbf{A} \mathbf{X}_i)$ .

Now let  $\mathbf{V}_i = (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_i)$  and  $\mathbf{R}_i = \mathbf{V}_i \mathbf{V}_i^T$ , the orthogonality constraint  $\mathbf{v}_j^T \mathbf{v}_i = 0, \forall 1 \leq j < i$  is equivalent to  $\|\mathbf{V}_{i-1}^T \mathbf{v}_i\|_2^2 = 0$ , and  $\|\mathbf{V}_{i-1}^T \mathbf{v}_i\|_2^2 = \mathbf{v}_i^T \mathbf{V}_{i-1} \mathbf{V}_{i-1}^T \mathbf{v}_i = \operatorname{Tr}(\mathbf{R}_{i-1} \mathbf{X}_i) = 0$ . Similarly as in [5], we relax  $\operatorname{Card}(\mathbf{X}_i) < k^2$  to  $\|\mathbf{X}_i\|_{1,1} < k$  and move it to the objective function with a coefficient  $\lambda$ . Finally, the non-convex constraint  $\operatorname{rank}(\mathbf{X}_i) = 1$  is dropped, and we have an objective function that can be solved by semidefinite programming (SDP) as in Eqn. 9.

$$\begin{aligned} & \underset{\mathbf{X}_i \in \mathbb{S}^p}{\operatorname{argmax}} \quad \operatorname{Tr}(\mathbf{A} \mathbf{X}_i) - \lambda \|\mathbf{X}_i\|_{1,1} \\ & \text{s.t. } \mathbf{X}_i \succeq 0, \operatorname{Tr}(\mathbf{X}_i) = 1, \operatorname{Tr}(\mathbf{R}_{i-1} \mathbf{X}_i) = 0 \end{aligned} \quad (9)$$

As  $\operatorname{rank}(\mathbf{X}_i)$  might not be 1, so we use the dominant eigenvector of  $\mathbf{X}_i$  as the approximate solution for  $\mathbf{v}_i$ .

### Solving ASPCA-B with SDP Relaxation.

To solve Eqn. 5, following the same steps above, we can get Eqn. 10, which is still a convex programming problem and can be solved by semidefinite programming (SDP).

$$\begin{aligned} & \underset{\mathbf{X}_i \in \mathbb{S}^p}{\operatorname{argmin}} \quad \operatorname{Tr}(\mathbf{A} \mathbf{X}_i) + \lambda \|\mathbf{X}_i\|_{1,1} \\ & \text{s.t. } \mathbf{X}_i \succeq 0, \operatorname{Tr}(\mathbf{X}_i) = 1, \operatorname{Tr}(\mathbf{R}_{i-1} \mathbf{X}_i) = 0 \end{aligned} \quad (10)$$

### Global Sparsity Optimization.

Let  $\mathbf{V} = (\mathbf{v}_1, \dots, \mathbf{v}_d)$  be the set of sparse loading vectors extracted by solving Eqn. 9 or Eqn. 10, which is also a set of basis vectors spanning the abnormal subspace. Notice that for any set of basis vectors  $\mathbf{c}_1, \dots, \mathbf{c}_d$  spanning the same subspace, we have

$$\operatorname{SPE} = \sum_{i=1}^d (\mathbf{v}_i^T \mathbf{y})^2 = \sum_{i=1}^d (\mathbf{c}_i^T \mathbf{y})^2 \quad (11)$$

Hence, we can employ a global sparsity optimization step to make the basis vectors of the same abnormal subspace sparser. To this end, we form the following optimization problem on an orthogonal transformation matrix  $\mathbf{X}$ ,

$$\begin{aligned} & \underset{\mathbf{X}}{\operatorname{argmin}} \quad \|\mathbf{V} \mathbf{X}\|_{1,1} \\ & \text{s.t. } \mathbf{X}^T \mathbf{X} = \mathbf{I} \end{aligned} \quad (12)$$

Let  $\mathbf{C} = \mathbf{V}\mathbf{X}$ , we transform this problem to the following regression problem,

$$\begin{aligned} \underset{\mathbf{X}, \mathbf{C}}{\operatorname{argmin}} \quad & \|\mathbf{V} - \mathbf{C}\mathbf{X}^T\|_F + \mu\|\mathbf{C}\|_{1,1} \\ \text{s.t.} \quad & \mathbf{X}^T\mathbf{X} = \mathbf{I} \end{aligned} \quad (13)$$

Eqn. 13 can be solved by using the alternating minimization scheme as in [23], with initial  $\mathbf{X}$  being an identity matrix. Initially, we set  $\mu = \|\mathbf{V}\|_F / \|\mathbf{V}\mathbf{X}\|_{1,1}$  to emphasize more on the sparsity objective, and gradually degrade  $\mu$  to a small value to ensure  $\mathbf{C}$  spanning the same subspace as  $\mathbf{V}$  through the last iterations.

Adding the global sparsity optimization step to ASPCA-F and ASPCA-B, we have two new models ASPCA-FG and ASPCA-BG, respectively. Algorithms 1 and 2 summarize the entire optimization process, where  $\mathbf{A}$  is the covariance matrix of the input dataset,  $d$  is the number of sparse principal components extracted from the abnormal subspace,  $\text{max\_iter}$  is the number of iterations for the global sparsity optimization, and the output loading matrix  $\mathbf{V}$  contains  $d$  orthogonal and sparse loading vectors for detecting and interpreting anomalies.

---

**Algorithm 1** Forward Abnormal Subspace Sparse PCA with Global Optimization (ASPCA-FG)

---

**Input:**  $\mathbf{A}$ ,  $d$ ,  $\lambda$ , and  $\text{max\_iter}$

**Output:**  $\mathbf{V}$

```

1: for  $i = 1$  to  $p$  do
2:    $\mathbf{V}_{i-1} \leftarrow (\mathbf{v}_1, \mathbf{v}_2 \dots \mathbf{v}_{i-1})$ ;
3:    $\mathbf{R}_{i-1} \leftarrow \mathbf{V}_{i-1}\mathbf{V}_{i-1}^T$ ;
4:   Optimize  $\mathbf{v}_i$  with given  $\mathbf{A}$ ,  $\mathbf{R}_{i-1}$  according to Eqn. 9
     using SDP;
5: end for
6:  $\mathbf{V} \leftarrow (\mathbf{v}_{p-d+1}, \dots, \mathbf{v}_p)$ ;
7: Optimize  $\mathbf{X}$ ,  $\mathbf{C}$  with given  $\mathbf{V}$ ,  $\text{max\_iter}$  according to
   Eqn. 13 using the alternating minimization scheme;
8:  $\mathbf{V} \leftarrow \mathbf{C}\mathbf{X}$ ;
9: return  $\mathbf{V}$ ;
```

---



---

**Algorithm 2** Backward Abnormal Subspace Sparse PCA with Global Optimization (ASPCA-BG)

---

**Input:**  $\mathbf{A}$ ,  $d$ ,  $\lambda$ , and  $\text{max\_iter}$

**Output:**  $\mathbf{V}$

```

1: for  $i = 1$  to  $d$  do
2:    $\mathbf{V}_{i-1} \leftarrow (\mathbf{v}_1, \mathbf{v}_2 \dots \mathbf{v}_{i-1})$ ;
3:    $\mathbf{R}_{i-1} \leftarrow \mathbf{V}_{i-1}\mathbf{V}_{i-1}^T$ ;
4:   Optimize  $\mathbf{v}_i$  with given  $\mathbf{A}$ ,  $\mathbf{R}_{i-1}$  according to Eqn. 10
     using SDP;
5: end for
6:  $\mathbf{V} \leftarrow (\mathbf{v}_1, \mathbf{v}_2 \dots \mathbf{v}_d)$ ;
7: Optimize  $\mathbf{X}$ ,  $\mathbf{C}$  with given  $\mathbf{V}$ ,  $\text{max\_iter}$  according to
   Eqn. 13 using the alternating minimization scheme;
8:  $\mathbf{V} \leftarrow \mathbf{C}\mathbf{X}$ ;
9: return  $\mathbf{V}$ ;
```

---

## 5. EXPERIMENT

### 5.1 Datasets

Our proposed ASPCA models were evaluated on the synthetic data introduced in Section 2, a medical dataset **Breast-Cancer**, and a network intrusion detection dataset **KDD99**.

**Breast Cancer Wisconsin (Diagnostic) Data Set** [1] provides features to distinguish malignant and benign tumors. The features describe characteristics of the cell nuclei present in a digitized image of a *fine needle aspirate* (FNA) of a breast mass. As there are plenty cells for a breast mass, the features are three important statistics (mean, standard error, and worst value) on 10 features for each cell: *radius*, *texture*, *perimeter*, *area*, *smoothness*, *compactness*, *concavity*, *concave points*, *symmetry* and *fractal dimension*. There are 357 benign records, and we kept the first 10 malignant records to transform the classification task to an anomaly detection task, same as the other works [14, 3] did. All 30 real-valued features were deducted by the mean values and linearly scaled to  $[-1, 1]$ .

**KDD 99 Intrusion Dataset** [2] is a widely used data for anomaly and intrusion detection. Each instance is a connection record classified as normal or one of 22 classes of attacks. Attacks fall into four main groups: DoS, Remote-to-local, User-to-root, and Probe. We chose all normal and part of the abnormal records in 10% KDD99 datasets as shown in Table 1 as picking the first 500 records on *smurf*, *neptune*, *back*, *teardrop*, *satant*, *ipsweep*, and *portsweep* and all records on other attacking types. The number of records for each type are shown in brackets in Table 1 too. We followed a similar preprocessing procedure as in [11]. There are 41 features including seven categorical features which were mapped into distinct positive integers from 0 to  $m-1$  ( $m$  is the number of states for the categorical feature). For example, 0 to 2 in *protocol\_type* stands for TCP, UDP, and ICMP. Logarithmic scaling was applied on *duration*, *src\_bytes*, and *dst\_bytes*, and all features were deducted by the mean values and linearly scaled to  $[-1, 1]$ .

### 5.2 Methodology

We compared our proposed ASPCA models with the standard PCA model for detection and sparsity performance, and with two state-of-the-art analytical models on PCA results: the JSPCA model [11] and a decision tree model used in [22] for interpretation performance. For the decision tree model, we formed the training set with all predicted normal records and anomalies returned by our ASPCA model as negative and positive samples, respectively. Then the decision trees were trained using the CART model from MATLAB and trimmed manually for the best interpretation.

The parameters used in our model were listed in Table 2 and discussed in Section 5.4. The number of PCs used in PCA equals the total number of features minus the number of abnormal PCs for all datasets. The results of JSPCA on the synthetic data were obtained by choosing the best performed parameters, and we directly reported their results on KDD99 in [11]. Note that, our ASPCA models make no assumptions on the anomalies in the dataset, and we built one model on the entire KDD99 dataset with anomalies from all different categories, whereas JSPCA built four models on KDD99, each including anomalies for a single major attacking category [11].

Finally, we implemented all methods with MATLAB and

**Table 1: Statistics of KDD99 and the relevant features identified by JSPCA**

Categories	# Records	Types	Relevant Features (JSPCA)
Normal	97,277		
DoS	2,264	smurf(500), neptune(500), back(500), teardrop(500), pod(264)	<i>service</i> , <i>src_bytes</i> , <i>dst_bytes</i> , <i>count</i> , <i>srv_count</i> , <i>dst_host_count</i> , <i>dst_host_srv_count</i>
Probe	1,731	satan(500), ipsweep(500), portsweep(500), nmap(231)	<i>source_bytes</i>
U2R	52	buffer_overflow(30), loadmodule(9), perl(3), rootkit(10)	<i>duration</i> , <i>src_bytes</i> , <i>dst_bytes</i> , <i>dst_host_count</i> , <i>dst_host_srv_count</i>
R2L	1,126	ftp_write(8), guess_passwd(53), imap(12), multihop(7), phf(4), spy(2), warezclient(1,020), warezserver(20)	<i>duration</i> , <i>service</i> , <i>src_bytes</i> , <i>dst_bytes</i> , <i>dst_host_count</i> , <i>dst_host_srv_count</i>

**Table 2: Parameters**

	# abnormal PCs	$\lambda$
Synthetic	4	5
Breast-Cancer	10	5
KDD99	35	100

CVX, and performed all experiments on a laptop computer with 16 GB memory and a Intel(R) Core(TM) i7-4870HQ 2.50GHz CPU.

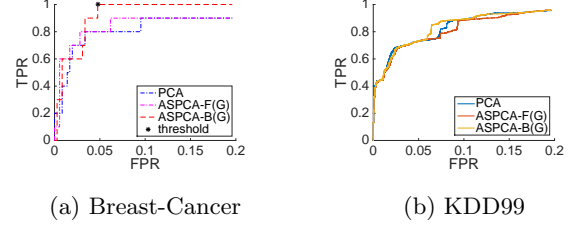
### 5.3 Experimental Results

#### 5.3.1 Detection Evaluation

We first compared the various ASPCA models with the standard PCA model on the anomaly detection performance. Because all models can obtain a perfect ROC curve for the Synthetic data, we only show the ROC curves on Breast-Cancer and KDD99 in Figure 3a and Figure 3b, respectively. Note that, since ASPCA-F and ASPCA-FG use the same abnormal subspace to detect anomalies, their ROC curves are identical which are labeled as ASPCA-F(G). Similarly, the ROC curves of ASPCA-B and ASPCA-BG are labeled as ASPCA-B(G). From Figure 3a, we can see that our proposed ASPCA-F(G) and ASPCA-B(G) models performed similarly or even better than PCA on anomaly detection for both datasets.

#### 5.3.2 Sparsity Evaluation

The next set of experiments were designed to compare the sparsity of the loading matrix generated by various ASPCA models and we used the result of PCA as our baseline. We used three metrics to evaluate the sparsity of the loading matrix of the abnormal PCs, namely,  $\|V\|_{1,1}$ ,  $Card_{0.1}$  (number of entries with absolute values bigger than 0.1), and  $Card_{0.01}$  (number of entries with absolute values bigger than 0.01), and showed the results in Table 3. We can see that all ASPCA models improved the sparsity of the



**Figure 3: ROC curves**

**Table 3: Sparsity on Synthetic data, Breast-Cancer, and KDD99**

dataset	method	$\ V\ _{1,1}$	$card_{0.1}$	$card_{0.01}$
Synthetic	PCA	7.07	16	24
	ASPCA-F	5.54	9	9
	ASPCA-B	5.31	8	8
	ASPCA-FG	5.54	9	9
Breast-Cancer	PCA	34.22	111	237
	ASPCA-F	17.23	33	50
	ASPCA-B	12.31	18	18
	ASPCA-FG	16.50	36	63
KDD99	PCA	97.33	248	691
	ASPCA-F	55.01	96	265
	ASPCA-B	54.52	101	215
	ASPCA-FG	42.77	58	159
	ASPCA-BG	43.05	57	157

loading matrix greatly over the baseline. For all datasets, the ASPCA-B model achieved better sparsity performance than the ASPCA-F model. The global optimization step improved  $\|V\|_{1,1}$  values for both models on Breast-Cancer and KDD99. However, in terms of cardinality, ASPCA-FG performed worse than ASPCA-F on Breast-Cancer. The global optimization step achieved the largest sparsity improvement on KDD99, as it has more abnormal PCs than the other two datasets leaving more room for the global optimization. Overall, the ASPCA-BG model achieved the best sparsity performance.

The loading matrices returned by PCA and ASPCA-B (the other three ASPCA models have very similar results) on the Synthetic data are shown in Figure 1, and the loading matrices returned by PCA, ASPCA-F, ASPCA-B, ASPCA-FG, ASPCA-BG on Breast-Cancer and KDD99 are shown in Figure 4. We can see that ASPCA-F usually leaves some loading vectors with poor sparsity towards the end, which should be avoided as they are part of abnormal subspace. On the contrary, ASPCA-B leaves the loading vectors not so sparse towards the beginning, which need no interpretation as they belong to the normal subspace.

#### 5.3.3 Interpretation Evaluation

Now we evaluate the interpretation performance of the ASPCA-BG model, as it has the best sparsity performance. Since we want to see how true anomalies are interpreted by our model, we selected a threshold value on SPE to ensure most of the true anomalies are detected. We show the threshold values, false positive rates (FPR), and true positive rates (TPR) for all three datasets in Table 4.

**Synthetic Data:** The four abnormal PCs and the pro-

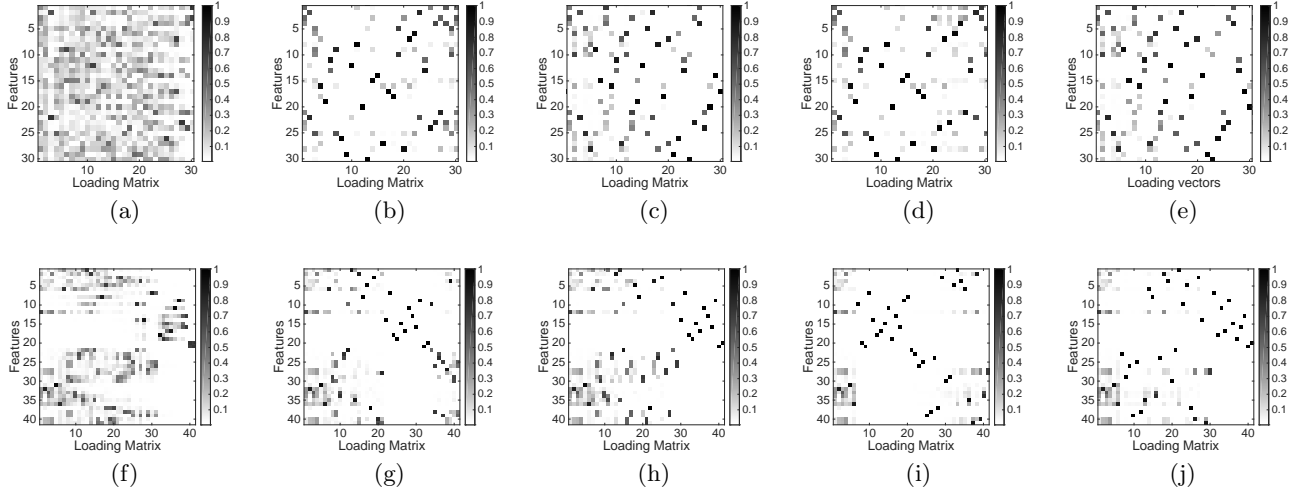


Figure 4: Loading matrix of PCs of Breast-Cancer (Top) and KDD99 (Bottom) obtained by PCA, ASPCA-F, ASPCA-B, ASPCA-FG, and ASPCA-BG from left to right

**Table 4: SPE Threshold**

	SPE threshold	TPR	FPR
Synthetic	0.25	1	0
Breast-Cancer	0.1003	1	0.0476
KDD99	0.5075	0.8516	0.0657

**Table 5: Components on Synthetic Data**

Index	Components
1	0.3099 A + 0.3122 B + 0.6370 C - 0.6330 D
2	0.7095 A - 0.7047 B
3	1 F
4	1 G

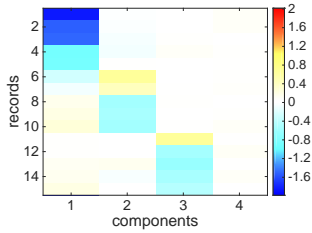


Figure 5: Heatmap of projection values of anomalies on abnormal PCs for Synthetic Data

jection values of 15 anomalies on these PCs are shown in Table 5 and Figure 5, respectively. As shown in Table 5, the first three PCs correspond to the rules of  $D \approx C + A$ ,  $A \approx B$ , and  $F \approx 0$ , respectively. The anomalies breaking these rules indeed have large projection values on the corresponding PCs. Thus, our ASPCA-BG model can not only identify the set of features that are responsible for an anomaly, but also tell the cause of the anomaly, i.e., breaking the rules indicated by the abnormal PCs.

JSPCA also successfully identified the relevant features ( $A, B, D, F$ ) as suggested in Figure 2. However, it cannot tell the source of each individual anomaly. Unlike JSPCA, our ASPCA models make no assumptions on whether there are anomalies present in the dataset for model training. Keeping only normal data from the Synthetic dataset, the ASPCA-BG model found four abnormal PCs with loading vectors  $(0.31, 0.31, 0.64, 0.64, 0, 0, 0)^T$ ,  $(-0.71, 0.71, 0, 0, 0, 0)^T$ ,  $(0, 0, 0, 0, 0, 1)^T$ , and  $(0, 0, 0, 0, 0, 0, 1)^T$ , which are very similar to the ones in Table 5. Using these abnormal PCs, we can successfully detect and interpret anomalies as well.

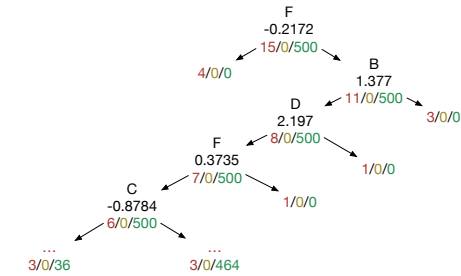


Figure 6: Decision tree on Synthetic Data

The decision tree was shown in Figure 6, where on each node we showed the feature and its value used to partition the data, the number of true positives detected by ASPCA-BG in red, the number of false positives in yellow, and the number of normal data detected by ASPCA-BG in green. We can see that the decision tree model needs several rules to describe a group of anomalies which could be easily described by a clear linear combination and a threshold. In Figure 6, only the third type of anomalies, which has a large absolute value on  $F$ , is easy for the decision tree model to interpret.

**Breast-Cancer:** The projection values of 10 anomalies on the abnormal PCs obtained by ASPCA-BG for Breast-Cancer are shown in Figure 7. We can see that the malignant records have two patterns: the first four records have large projection values on the 2nd, 3rd, and 4th PCs, the rest records have large projection values on the first PC and moderate projection values on the 6th PC. We show these



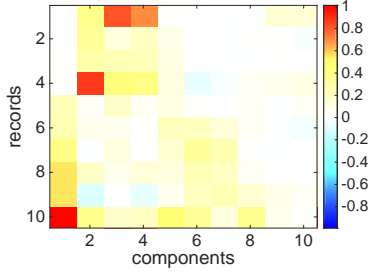


Figure 7: Heatmap of projection values of anomalies on abnormal PCs of Breast-Cancer

Table 6: Components on Breast-Cancer.

Index	Components
1	1 <i>area_se</i>
2	0.9894 <i>symmetry_worst</i>
3	0.9631 <i>fractal_dimension_worst</i> - 0.2693 <i>fractal_dimension_mean</i>
4	0.9445 <i>compactness_worst</i> - 0.3286 <i>compactness_mean</i>
6	0.8554 <i>area_worst</i> - 0.5180 <i>radius_worst</i>

PCs in Table 6, where coefficients in PCs less than 0.1 were omitted. The features appearing in the 1st and 6th PCs are *area\_se*, *area\_worst*, and *radius\_worst*, which were reported previously by [20] as being effective for classifying malignant records. Note that, *area\_worst* actually has a quadratic relation with *radius\_worst*, our model identified it as a linear relation, which is a good approximation in a small range of radius. The first four records, on the other hand, do not have large projection values on PCs related to *area* features. They were detected by PCs related to *symmetry*, *fractal dimension*, and *compactness* features, which clearly indicates another type of malignant records.

The loading matrix of the abnormal PCs obtained by JSPCA on Breast-Cancer is shown in Figure 8. The relevant features are *radius\_mean*, *concavity\_mean*, *area\_se*, *fractal\_dimension\_se*, *perimeter\_worst*, and *compactness\_worst*. As we can see, JSPCA cannot tell the different causes of individual anomalies. The decision tree obtained on Breast-Cancer is shown in Figure 9. Our ASPCA-BG model detected 10 true positives, 18 false positives, and 339 true negatives (shown on the root node in red, yellow, and green, respectively) with the chosen SPE threshold. The tree used *concavity\_mean* to separate positive and negative samples. However, the attribute *concavity\_mean* is orthogonal to the abnormal subspace obtained by our ASPCA-BG model, which

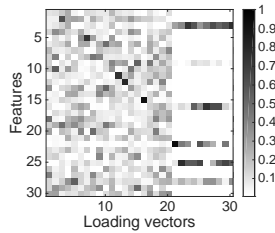


Figure 8: Loading matrix of abnormal PCs obtained by JSPCA on Breast-Cancer

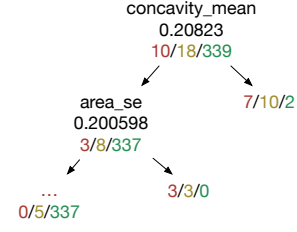


Figure 9: Decision tree on Breast-Cancer

Table 7: Signatures on KDD99

Type	# in Type/ # in Group	Important Components
neptune[DoS] 500/500	481/484	2L, 9H, 10H 11H, 12H, 14H
smurf[DoS] 493/500	472/472	1H, 3L, 8H, 16H
teardrop[DoS] 496/500	393/393	18H
satan[Probe] 500/500	444/444	2L, 3H, 6H, 8H
portsweep[Probe] 354/500	175/175	6H, 7L
ipsweep[Probe] 217/500	104/109	1H, 19H
warezclient[R2L] 974/1020	272/395 332/339 237/292	15H, 20H 4L, 5H, 6L 4L, 5H
guess-passwd[R2L] 53/53	48/121	4H, 5H
buffer-overflow[U2R] 30/30	7/7	5H, 24H

means it is not the feature based on which our ASPCA-BG model detects anomalies. Hence, using decision trees to interpret results of a subspace-based model, such as ours, may lead to misleading interpretations.

**KDD99:** With the given SPE threshold, our ASPCA-BG model detected 4397 true positives on KDD99. Although our model is intended to analyze individual anomalies, we can also summarize interpretations of similar anomalies to make our discussion easier. We used a simple way to generate signatures on whether an anomaly has *low* ( $\leq -\sqrt{SPEthreshold}/2$ ), or *high* ( $\geq \sqrt{SPEthreshold}/2$ ) projection values on the set of abnormal PCs. Then anomalies were grouped according to their signatures, so that the components in the signature of each group is common for most of the anomalies in the group.

In Table 7, we listed some major signatures found by the above method. Actually, for most of the cases, we can associate each signature group with an anomaly type quite well. The two numbers listed for each anomaly type are the number of detected anomalies by our model and the number of total anomalies of this type, respectively. The two numbers listed for each signature group are the number of the anomalies of this type and the total number of anomalies in the group, respectively. Some anomaly types only have one main corresponding signature groups, whereas we identified three main signature groups for warezclient[R2L]. For the  $i$ th PC,  $iL$  and  $iH$  represent low and high projection values on it, respectively. Finally, the components appeared in these signatures are shown in Table 8.



Table 8: Components on KDD99

Index	Components
1	0.8906 <i>protocol_type</i> + 0.3658 <i>logged_in</i>
2	0.9949 <i>same_srv_rate</i>
3	0.9958 <i>diff_srv_rate</i>
4	0.9520 <i>dst_bytes</i> - 0.2222 <i>logged_in</i>
5	0.7722 <i>dst_host_same_srv_rate</i> - 0.6286 <i>dst_host_srv_count</i>
6	0.9466 <i>dst_host_diff_srv_rate</i>
7	0.9714 <i>duration</i>
8	0.9995 <i>count</i>
9	0.9716 <i>flag</i>
10	0.9984 <i>dst_host_error_rate</i>
11	0.9981 <i>srv_error_rate</i>
12	0.9981 <i>error_rate</i>
14	0.9985 <i>dst_host_srv_error_rate</i>
15	0.9997 <i>is_guest_login</i>
16	0.9994 <i>srv_count</i>
18	0.9996 <i>wrong_fragment</i>
19	0.9970 <i>dst_host_srv_diff_host_rate</i>
20	0.9999 <i>hot</i>
24	1 <i>root_shell</i>

From Table 7, we can see that the signatures for different anomaly types varied a lot, from which we often can find the components that are consistent with the nature of each anomaly type. For example, smurf[DoS] attacks are also known as popular form of DoS packet floods, which turn out to have high *srv\_count* and *count* values (*i.e.*, 16H and 8H). Teardrop[DoS] attacks try to break the host by sending mangled IP fragments, which led to high *wrong\_fragment* values (*i.e.*, 18H). We can see similar trends for Probe attacks too. For example, ipsweep[Probe] attacks sweep different hosts (IPs) to find cracks for hacking (*i.e.*, 19H), whereas portsweep[Probe] attacks try to visit different service (*i.e.*, 6H) and short connection duration (*i.e.*, 7L). Buffer overflow[U2R] attackers try to gain the root authority on the host, and 24H indicates that the user has logged into the server with root shell. Warezclient[R2L] attackers try to download files in forbidden directories from the FTP servers. Our interpretation is consistent with [18] as *logged\_in* with low *dst\_bytes* (*i.e.*, 4L), *is\_guest\_login* (*i.e.*, 15H) and high *hot* values (*i.e.*, 20H).

The results obtained by JSPCA are shown in Table 1. The selected features by JSPCA are more general and similar for all categories. Some of the important features for specific attacks are missing too, for instance, *root\_shell* for User-2-Root[U2R] attacks and *hot* and *is\_guest\_login* for R2L attacks as mentioned in [18].

We show the decision tree obtained on KDD99 in Figure 10. The features captured by the decision tree are consistent with the components discovered by our ASPCA-BG model to a large extent. For example, low *same\_srv\_rate* was chosen to detect neptune and satan DoS attackers, which is the same as using 2L in our model to detect the same attacks. Similarly, high *protocol\_type* values (*i.e.*, using ICMP protocol) was chosen to detect ipsweep and smurf attackers (detected by 1H in our model). Low *dst\_host\_srv\_count* with high *hot* values is an important character of warezclient and guess-passed attacks (identical to 5H and 20H in our model). An interesting observation on the decision tree in Figure 10 is that a node on the tree will stop splitting as soon as the samples in the node are mostly positive or

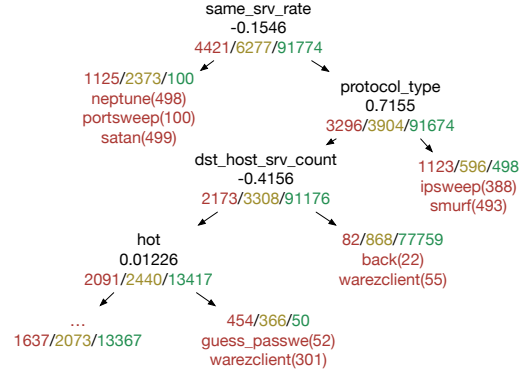


Figure 10: Decision tree on KDD99

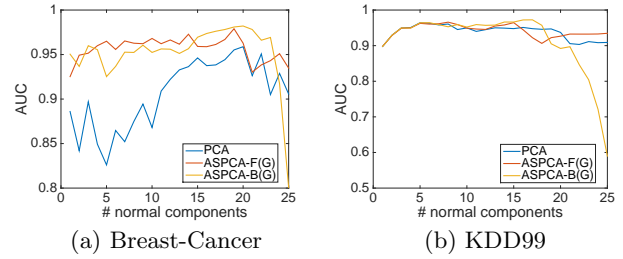


Figure 11: Selection on the number of normal PCs

negative ones. For example, the left child node of the root in Figure 10 stopped splitting with anomalies from different attack types, in which case, our model can provide more information on the differences of these attack types.

## 5.4 Parameter Selection

Our ASPCA models have two parameters to select: the number of abnormal PCs and the coefficient  $\lambda$  on sparsity. We know that PCA-based anomaly detection methods are sensitive to the number of PCs [17]. We plotted the detection accuracy (in terms of Area Under ROC Curve (AUC)) with different number of abnormal PCs on Breast-Cancer (with  $\lambda = 5$ ) and KDD99 ( $\lambda = 100$ ) in Figure 11. We selected 20 normal PCs (*i.e.*, 10 abnormal PCs) for Breast-Cancer data and 6 normal PCs (*i.e.*, 35 abnormal PCs), for KDD99 data, to achieve the highest AUC values for our baseline method PCA, to make the comparisons on detection accuracy fair.

The coefficient  $\lambda$  is a trade-off between the sparsity and the additional variance on components. With less additional variance, the variances on the whole detection space for various ASPCA models are closer to the one of PCA. We showed the variance, sparsity (valued by  $\|V\|_{1,1}$ ) and AUC values obtained by varying the value of  $\lambda$  on KDD99 and Breast-Cancer in Table 9 for ASPCA-FG and ASPCA-BG. We can see that our models are not very sensitive to  $\lambda$  in terms of AUC, and we selected  $\lambda = 5$  for Breast-Cancer,  $\lambda = 100$  for KDD99 for moderate sparsity and variance. The trends are similar for ASPCA-F and ASPCA-B, which were omitted due to space constraints. We selected the same  $\lambda$  values for ASPCA-F and ASPCA-B, as in ASPCA-FG and ASPCA-BG, respectively.

Table 9: Selection on  $\lambda$ 

ASPCA-FG				ASPCA-BG			
$\lambda$	$\ V\ _{1,1}$	Variance	AUC	$\ V\ _{1,1}$	Variance	AUC	
0	97.33	21518	0.963	97.33	21518	0.963	
10	44.38	21524	0.963	44.59	21523	0.963	
50	43.52	21627	0.962	43.97	21589	0.964	
100	42.77	21873	0.960	43.04	21735	0.964	
500	41.04	23673	0.956	40.67	22997	0.967	

(a) KDD99

ASPCA-FG				ASPCA-BG			
$\lambda$	$\ V\ _{1,1}$	Variance	AUC	$\ V\ _{1,1}$	Variance	AUC	
0	34.23	1.2728	0.959	34.23	1.2728	0.959	
1	26.68	14.2012	0.903	14.95	6.2777	0.950	
5	16.50	20.8308	0.963	12.31	20.2968	0.982	
10	12.81	30.8123	0.985	10	57.0009	0.966	
50	10	57.0009	0.966	10	57.0009	0.966	

(b) Breast-Cancer

## 6. CONCLUSIONS AND FUTURE WORK

Traditional PCA-based anomaly detection models are not suitable for anomaly interpretation, limiting its usage in the domains where interpretation is essential. In this paper, we found that the sparsity and orthogonality of the loading vectors are the keys to anomaly interpretation, and proposed an interpretable PCA-based anomaly detection model, the ASPCA model. We designed *forward* and *backward* ASPCA models and evaluated them on two real world datasets. Our model achieved similar or even better anomaly detection performance as the traditional PCA model, and provided meaningful interpretation for individual anomalies. Our future works will focus on three directions: 1) how to improve efficiency on high dimensional datasets; 2) how to extend our model to robust PCA for better detection performance; 3) how to extend our model to kernel PCA.

## 7. ACKNOWLEDGEMENT

This work is funded by the National 863 Program of China (Grant No. 2015AA01A301).

## 8. REFERENCES

- [1] Breast Cancer Wisconsin (Diagnostic) Data Set, 1995.
- [2] KDD Cup 1999 Data, 1999.
- [3] M. Amer, M. Goldstein, and S. Abdennadher. Enhancing one-class support vector machines for unsupervised anomaly detection. In *Proceedings of the ACM SIGKDD Workshop on Outlier Detection and Description*, ODD '13, pages 8–15. ACM, 2013.
- [4] V. Chandola, A. Banerjee, and V. Kumar. Anomaly Detection: A Survey. *ACM Computing Surveys*, 41(3):1–58, 2009.
- [5] A. d’Aspremont, L. El Ghaoui, M. I. Jordan, and G. R. G. Lanckriet. A Direct Formulation for Sparse PCA Using Semidefinite Programming. *SIAM Review*, 49(3):434–448, 2007.
- [6] R. Dunia and S. Joe Qin. Subspace approach to multidimensional fault identification and reconstruction. *AICHE Journal*, 44(8):1813–1831, 1998.
- [7] R. Fujimaki, T. Yairi, and K. Machida. An Approach to Spacecraft Anomaly Detection Problem Using Kernel Feature Space. In *Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining*, pages 401–410. ACM, 2005.
- [8] L. Huang, X. Nguyen, M. Garofalakis, J. M. Hellerstein, M. I. Jordan, A. D. Joseph, and N. Taft. Communication-Efficient Online Detection of Network-Wide Anomalies. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, pages 134–142. IEEE, 2007.
- [9] L. Huang, X. Nguyen, M. Garofalakis, M. I. Jordan, A. Joseph, and N. Taft. In-network PCA and anomaly detection. In *Advances in Neural Information Processing Systems*, pages 617–624. MIT Press, 2006.
- [10] R. Jiang, H. Fei, and J. Huan. Anomaly Localization for Network Data Streams with Graph Joint Sparse PCA. In *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 886–894. ACM, 2011.
- [11] R. Jiang, H. Fei, and J. Huan. A family of joint sparse pca algorithms for anomaly localization in network data streams. *Knowledge and Data Engineering, IEEE Transactions on*, 25(11):2421–2433, 2013.
- [12] I. Jolliffe. *Principal component analysis*. Wiley Online Library, 2002.
- [13] I. T. Jolliffe, N. T. Trendafilov, and M. Uddin. A Modified Principal Component Technique Based on the LASSO. *Journal of Computational and Graphical Statistics*, 12(3):531–547, 2003.
- [14] H.-P. Kriegel, P. Kröger, E. Schubert, and A. Zimek. Loop: Local outlier probabilities. In *Proceedings of the 18th ACM Conference on Information and Knowledge Management*, pages 1649–1652. ACM, 2009.
- [15] A. Lakhina, M. Crovella, and C. Diot. Diagnosing Network-wide Traffic Anomalies. In *Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 219–230. ACM, 2004.
- [16] A. Lakhina, M. Crovella, and C. Diot. Mining Anomalies Using Traffic Feature Distributions. In *Proceedings of the 2005 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 217–228. ACM, 2005.
- [17] H. Ringberg, A. Soule, J. Rexford, and C. Diot. Sensitivity of PCA for Traffic Anomaly Detection. In *Proceedings of the 2007 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, pages 109–120. ACM, 2007.
- [18] M. Sabhnani and G. Serpen. KDD Feature Set Complaint Heuristic Rules for R2L Attack Detection. In *International Conference in Computer Security and Management*, pages 310–316. Citeseer, 2003.
- [19] W. Wang and R. Battiti. Identifying intrusions in computer networks with principal component analysis. In *The First International Conference on Availability, Reliability and Security*, pages 270–279. IEEE, 2006.
- [20] W. H. Wolberg, W. Street, D. M. Heisey, and O. L. Mangasarian. Computer-derived nuclear features distinguish malignant from benign breast cytology. *Human Pathology*, 26(7):792 – 796, 1995.
- [21] W. Xu, L. Huang, A. Fox, D. Patterson, and M. Jordan. Experience mining Google’s production console logs. *Proceedings of the 2010 workshop on Managing systems via log analysis and machine learning techniques*, 2010.
- [22] W. Xu, L. Huang, A. Fox, D. Patterson, and M. I. Jordan. Detecting Large-scale System Problems by Mining Console Logs. In *Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles*, pages 117–132. ACM, 2009.
- [23] H. Zou, T. Hastie, and R. Tibshirani. Sparse Principal Component Analysis. *Journal of Computational and Graphical Statistics*, 15(2):265–286, 2006.